LastPass Migration to Dashlane - Technical Details

Last Modified on 04/22/2025 6:03 pm EDT

This article supplements the main announcement about migrating your LastPass account to the new Dashlane password management service. We recommend you start with University Retires LastPass Password Manager, and use this article if you run into trouble with those directions or if you need a more in-depth understanding of the nuances around the migration. This article repeats some of that information, and may be too much information for most people.

Types of University Accounts

There are several types of accounts.

LastPass Enterprise accounts

Enterprise Accounts include the option to create shared folders, which many teams use to share access credentials for software and other sensitive information. Only some Wharton staff and some faculty have LastPass Enterprise accounts. If you have a LastPass Enterprise account:

LastPass Premium personal accounts

Premium Accounts are personal LastPass accounts created for individual and personal use, taking advantage of the University's premium level of service. Various members of the University community have been eligible for a LastPass Premium account. If you have a LastPass Premium account, please see below for details:

> **Note**: The instructions provided by Dashlane say that disabling 2FA / two-factor authentication is required for the direct import to work. However, in testing, both Wharton Computing and ISC users have successfully imported their LastPass credentials with 2FA enabled. Using the same browser that you have the LastPass browser plugin already installed, or a LastPass session already running, should eliminate the need for disabling 2FA.

If you need to migrate a LastPass Shared folder: Dashlane Premium is probably not the right choice for you. Dashlane Premium does not allow for the ability to share password folders or collections. You can share individual password items, if that is sufficient for your purpose.

Further documentation is available at ISC's Dashlane documentation site.

LastPass Linked Account Users

This section applies to enterprise users who have linked their LastPass accounts to their personal accounts only.

Some users have their personal LastPass accounts to their Enterprise accounts. For example, jwharton@wharton.upenn.edu could have as Wharton enterprise account, and link their personal account under

the email jwharton@gmail.com. This gives users the advantage of having all of their passwords, for both business and personal use, accessible through the LastPass app, browser plugin, etc, through their single Enterprise login. You can check if you have any linked account settings enabled in the menu :

LastPass Free Account

If you don't fall into any of the account types above, you likely have a free LastPass account and won't be affected by this migration.

Migration Options

This chart reviews in depth the various options you have available, and reasons for choosing each option.

Current Last Pass Feature/Function Usage	Option 1: Keep LastPass Free Personal Account	Option 2: Migrate to Dashlane Premium	Option 3: Migrate to Dashlane Business Plan
LastPass account only for personal use	x		
Keep and use shared folders in your LastPass account.	x		x
Make use of premium features of password manager.		x	x
Wharton faculty or staff, and a current member of the Wharton LastPass Enterprise account.		x	x

Current Last Pass Feature/Function Usage	Option 1: Keep LastPass Free Personal Account	Option 2: Migrate to Dashlane Premium	Option 3: Migrate to Dashlane Business Plan
Use LastPass premium account to store University credentials or to collaborate and share passwords with other University employees.			x
Share credentials or access shared credentials with other Dashlane Business users.			x

Migrate to Wharton's Dashlane Business Plan

Dashlane Business accounts allow for the option to share credentials with other users and other advanced features.

Migrating a LastPass Shared folder (LastPass Enterprise users only)

You **must** export a .csv file of passwords from LastPass and then import the file directly into Dashlane. This has the downside of creating a plaintext .csv file containing passwords but allows for the export and transfer of any passwords a user had access to in LastPass, including from shared password folders, so care is required to ensure protection of your credentials.

When migrating a Shared LastPass folder: We recommend appointing **one** person that manages your Shared LastPass vault to be designated the **owner** of -- and thus responsible for -- the migration of the LastPass vault to a Dashlane collection (what a shared folder is called in Dashlane), then assigning shared access rights after the migration.

Always share collections with full "Manager" permissions, and add passwords with "Full" edit rights, so that even if the original creator loses access to their Dashlane account, subsequent managers can still retain full access to the shared folder.

Renewing LastPass Premium

If your LastPass Premium access expires before September 26, you should receive an email from LastPass about 2 weeks before your expiration date with the subject "Another year of LastPass, free!" Look for this email in your @upenn.edu account, and follow the instructions to open a link and renew access. (Be sure to use a browser that is set up to use your LastPassPremium account.)

LastPass Support has assured Penn that Premium Account users can continue to renew their LastPass license before September 26, so you should have full premium support until then. **After September 26, accounts may transition to free status so we recommend preparing in advance.**

Notes on Migrating Shared Folders

- **Sharing permissions from LastPass are NOT retained**. The person doing the sharing will have to reassign permissions. We recommend sharing with Manager permissions (for collections) and Full Access (for each credential) so Dashlane users can manage collections that are shared to them.
- **Nested folders get separated** out into their own collections. Either flatten your LastPass folder structure before the migration, or be prepared to deal with many Collections.
- **The import process may fail to import all shared folder/collection relationships**. We recommend uploading one shared Lastpass folder at a time by splitting it up into multiple CSV files so that you can verify the data you are uploading one collection at a time.
- **Credentials are** ALWAYS tied to the original account that created it. To share a password, you must:
  - create the password in your OWN personal login
  - add it to a shared collection

Always share collections with full "Manager" permissions, and add passwords with "Full" edit rights, so that even if the original creator loses access to their Dashlane account, subsequent managers can still retain full access to the shared folder.

Optional Actions:

Request a Dashlane Group to manage your shared passwords: You can request the creation of a Dashlane group to help manage your shared passwords. Members of a Dashlane group can share logins, Secure Notes, and secrets with other members of the group. See Dashlane's information on managing Dashlane groups. If you would like to create a Dashlane group or update the membership of a Dashlane group, please contact your Wharton Computing representative.

Lock down access to LastPass shared folder: Once you have migrated your collections to Dashlane, you can lock down access to your old LastPass shared folders to Read-Only access so that your team no longer makes edits and changes to the old LastPass shared folder.

Questions?

If you have trouble figuring out what kind of account you have, or need help with the migration process, please contact your Wharton Computing representative.

For more information on Dashlane, see ISC's website.